

Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) EP 0 965 903 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
22.12.1999 Bulletin 1999/51

(51) Int Cl.⁶ G06F 1/00

(21) Application number: 99304600.2

(22) Date of filing: 14.06.1999

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(72) Inventor: Drew, Colin
Dundee, Scotland, DD3 0QF (GB)

(74) Representative: Cleary, Fidelma et al
International IP Department
NCR Limited
206 Marylebone Road
London NW1 6LY (GB)

(30) Priority: 16.06.1998 GB 9812836

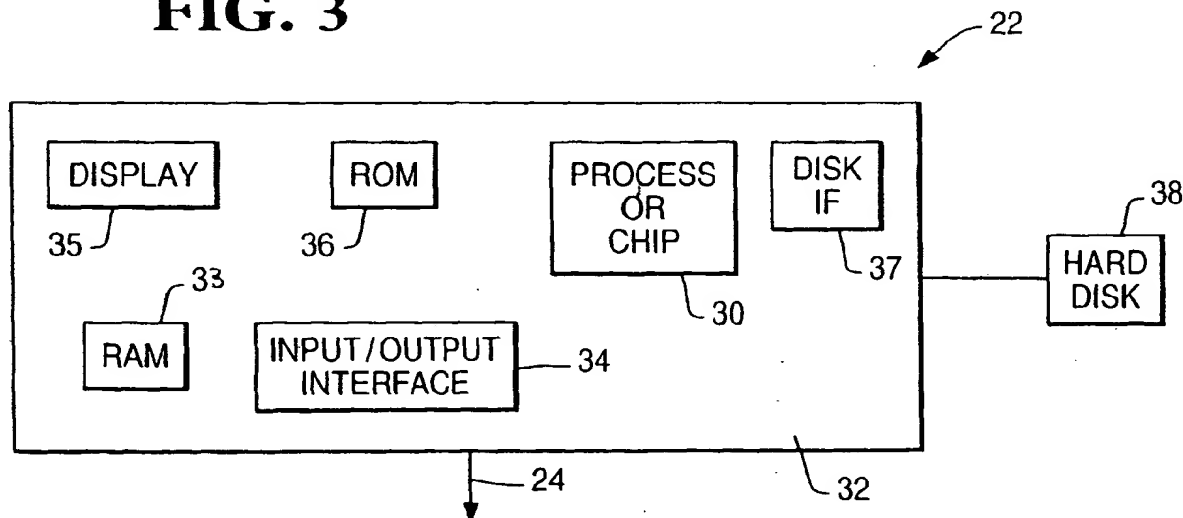
(71) Applicant: NCR INTERNATIONAL INC.
Dayton, Ohio 45479 (US)

(54) Data security arrangement

(57) An automated teller machine includes a processor (22) on a motherboard (32) with BIOS on ROM which allows operation of a hard disk (38) via an inter-

face (37). The disk has at least one normal partition and includes a hidden security partition inaccessible under normal system control. Data relating thereto can be encoded for security reasons.

FIG. 3



EP 0 965 903 A1

Description

[0001] The present invention relates to data security arrangements.

[0002] When handling data, for example, in a self service terminal such as an Automated Teller Machine (ATM), access needs to be restricted. When data is stored on a rotatable storage medium (e.g. a hard disk) there is a need to reduce the risk of unauthorized access.

[0003] The present invention is concerned with assisting in providing such security.

[0004] To this end, the invention consists in a security method for a rotatable storage device characterized by providing a hidden security partition in the device, and storing information on the position of the partition on the device in such a manner as to prevent access by normal system operation.

[0005] In a preferred embodiment, the method is employed in operating a self service terminal.

[0006] The invention also consists in a rotatable storage device having a storage sector for storing information on at least one storage partition and characterized by a hidden security partition located thereon and inaccessible during normal system operation.

[0007] In a preferred embodiment, the device is employed in a self service terminal.

[0008] In order that the present invention may be more readily understood, reference will now be made, by way of example, to the accompanying drawings, in which:-

Figure 1 shows a known ATM system;

Figure 2 shows the control system for the Figure 1 arrangement;

Figure 3 shows the processor control aspect of an ATM in more detail;

Figure 4 shows a typical partition table sector associated with the hard disk of Figure 3;

Figure 5 shows the inventive aspect of the hidden partition; and

Figure 6 shows the store and access mechanisms respectively for the hidden partition.

[0009] In the typical ATM arrangement of Figure 1 of the accompanying drawings, the ATM 10 is enclosed within a cabinet 11 and has customer utilization arrangements, such as a magnetic card input slot 12, a display screen 14, a keypad 16, a cash delivery slot 18 and a balance and/or payout slip delivery slot 19.

[0010] The control system for the ATM 10 is shown in Figure 2 in which a processor 22 is connected to receive input from the card reader 12 and the keypad 16 and control the display 14 and cash counting and delivery system 26 connected to the cash delivery slot 18. A paper slip delivery system 20 is provided for dispensing a printed payout slip, account balance or the like, and is connected to the delivery slot 19. The processor is con-

nected by a connector 24 to the central authorization system of the financial institution operating the ATM 10.

[0011] In the Figure 2 arrangement it is necessary to access, handle and store data and the processor arrangement 22 is shown in more detail in Figure 3. Typically the processor will include a number of components to allow the system to operate. The heart of the processor will be a microprocessor chip 30 mounted on a motherboard 32. Input and output information/control will pass via an interface 34 and driving the display will be achieved by the display driver 35. Memory chips 33 (RAM) provide immediate data handling capability.

[0012] Other memory chips 36 (ROM) provide operational information in permanent form. A disk interface 37 provides connection to a hard disk 38 through its disk controller (not shown separately).

[0013] The devices, except the hard disk 38, are all shown mounted on the motherboard for simplicity, but some devices may be situated on separate cards mounted on the motherboard.

[0014] A hard disk 38 provides large scale storage for the computer and will carry software to run the system as well as data regarding transactions and the like. The motherboard BIOS (Basic Input Output System) allows the system to operate correctly including hard disk operation. This BIOS is accessed at the commencement of the boot up program and the BIOS is typically held in the ROM 36 (and possibly partially in the disk controller).

[0015] For the computer to bootstrap (boot) after internal self checks, the ROM BIOS checks the hard drive at a specific location for 'system files' and reads data stored on the disk's first sector and copies this to RAM to allow the stored system files to be loaded into RAM.

[0016] During the computer system operation, when data is to be read from a file, the operating system instructs the hard disk controller to move the drive head to the drive's file allocation table (FAT) to determine where the start of that file begins so that the correct file can be accessed.

[0017] Security of information on ATMs is paramount to both the Financial Institutions and the customer in the street. To protect this information system/procedures require to be in place to restrict/control access to the software and data present on the ATM's hard drive 38. This includes restricting system boot up if certain security criterion are not met.

[0018] During the normal software initialization of a hard disk, partitions are laid down in the first sector of a disk, known as the Partition Table Sector. Within this first sector there is a defined area called the Partition Table where up to four 16 byte partition entries can be written. This information details where each partition is located on the disk, how big it is and whether the partition can be used to boot the system. The Motherboard BIOS within the system indexes into this Partition Table to find the boot partition and then loads the boot sector code pointed to by the boot partition and subsequently loads

the system software. A typical Partition Table Sector from a disk is shown in Figure 4.

[0019] The Partition Table Sector has a storage capacity of 16 x 32 (512 bytes). The bootstrap code is at the beginning (commencing at address 00000000) with Partition Table entries towards the end of the sector. Each Partition Table entry requires 16 bytes of data. As illustrated the first Partition Table entry (shown in bold) commences as address 000001B0. Up to four partitions may be required on large disks and each 16 byte entry can follow on from each other up to the end of the sector. Thereafter bytes '55 AA' denote to the computer BIOS that the Partition Table contains valid data.

[0020] With the present invention, a Security Partition is included above the area where the standard partition entry information is placed, utilizing space within the Partition Table Sector, so that it will not be recognized by the normal operating system as a hidden partition.

[0021] The Security Partition data details the whereabouts of the special hidden partition on the disk. Since Operating Systems currently only use the defined Partition Table area to detail partition information, the Security Partition would be unknown and therefore inaccessible to other users. The Security Partition details can also be encoded such that it was not obvious that the data was describing a hidden disk partition. This hidden partition can then contain proprietary code and information used to implement secure access to the system software and data.

[0022] Figure 5 again shows a partition table but it now includes hidden Security Partition data within the Partition Table Sector. The normal partition information is again written at address 000001B0. However, unused space above the area recognized as giving partition information is employed for security partition data. In this example the offset address 00000160 is used and data indicative of the partition is stored (shows as XX bytes). Only knowledge of the offset of the hidden Security Partition data entry within the Partition Table Sector and the encoding algorithm would allow the hidden partition to be found.

[0023] Hence, to set up the Security Partition, the appropriate partition defining information can be laid down at the offset address by means of the steps shown in Figure 6a. Access can be made using the steps shown in Figure 6b, which is outside the accessibility of the normal operating system.

[0024] During installation of the ATM build suite, the Partition Table Sector would be written with the encoded hidden Security Partition. Only the manufacturer's proprietary software/firmware would have knowledge of the encoding algorithm and the offset address of the hidden partition data. The software load of data onto the disk could include loading any security information into the hidden partition on the disk, access to which would only be achieved through special proprietary software and firmware routines. The motherboard BIOS could also be modified to include special routines to access the hidden

partition to validate security data before allowing the system to boot.

[0025] Hence, this additional security measure restricts/controls access to the software and data on the hard disk and includes restricting system boot up if certain security requirements are not met.

[0026] In the arrangement shown in Figure 3, the disk 38 is an IDU disk. In a variation, for use with an SCSI disk, the disk interface 37 is replaced by an SCSI controller.

Claims

1. A security method for a rotatable storage device (38), characterised by the steps of providing a hidden security partition in the device, and storing information on the position of the hidden partition on the device in such a manner as to prevent access by normal system operation.
2. A method according to claim 1, characterised in that the hidden partition position information is stored at a location remote from information relating to any non-security partition.
3. A method according to claim 1 or 2, characterised in that the hidden partition position information is stored in a partition table at a location away from other non-security partition information within the same partition table.
4. A method according to claim 1, 2 or 3, characterised in that the information on the hidden partition is security encoded prior to storage to prevent interpretation even when subject to unauthorized access.
5. A method according to any preceding claim, characterised in that the method is utilised in the operation of a self-service terminal having a rotatable storage device.
6. A rotatable storage device (38) comprising a storage sector for storing information on at least one storage partition, characterised in that the storage sector has a hidden security partition located thereon and inaccessible during normal system operation.
7. A rotatable storage device according to claim 6, characterised in that position information on the hidden security partition is stored at a location remote from information relating to any non-security partitions.
8. A rotatable store device according to claim 6 or 7, characterised in that information on the hidden security partition is security encoded to prevent inter-

pretation in the event that it is subject to unauthorized access.

9. A self-service terminal comprising a processor (22), a display (14) and a dispenser (26) operable in response to an authorized user request, characterised by a rotatable storage device (38) as claimed in claim 6, 7 or 8. 5
10. A self-service terminal according to claim 9, characterised in that the self-service terminal comprises an automated teller machine and the dispenser (18) is operable to dispense cash in response to an authorized user request. 10

15

20

25

30

35

40

45

50

55

FIG. 1

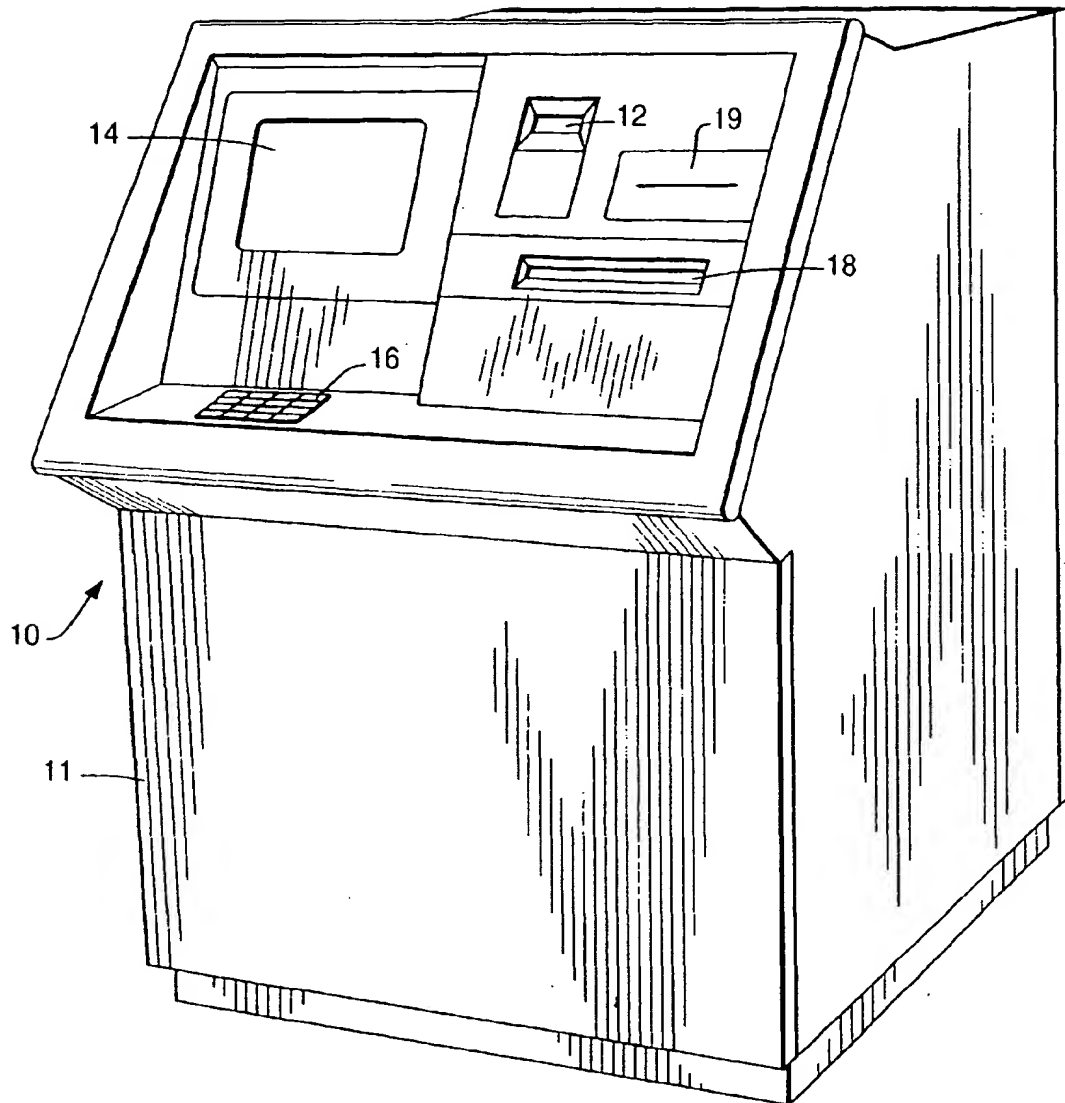


FIG. 2

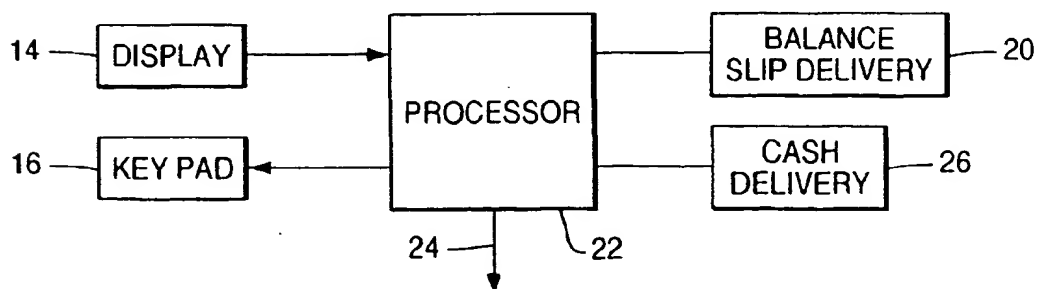
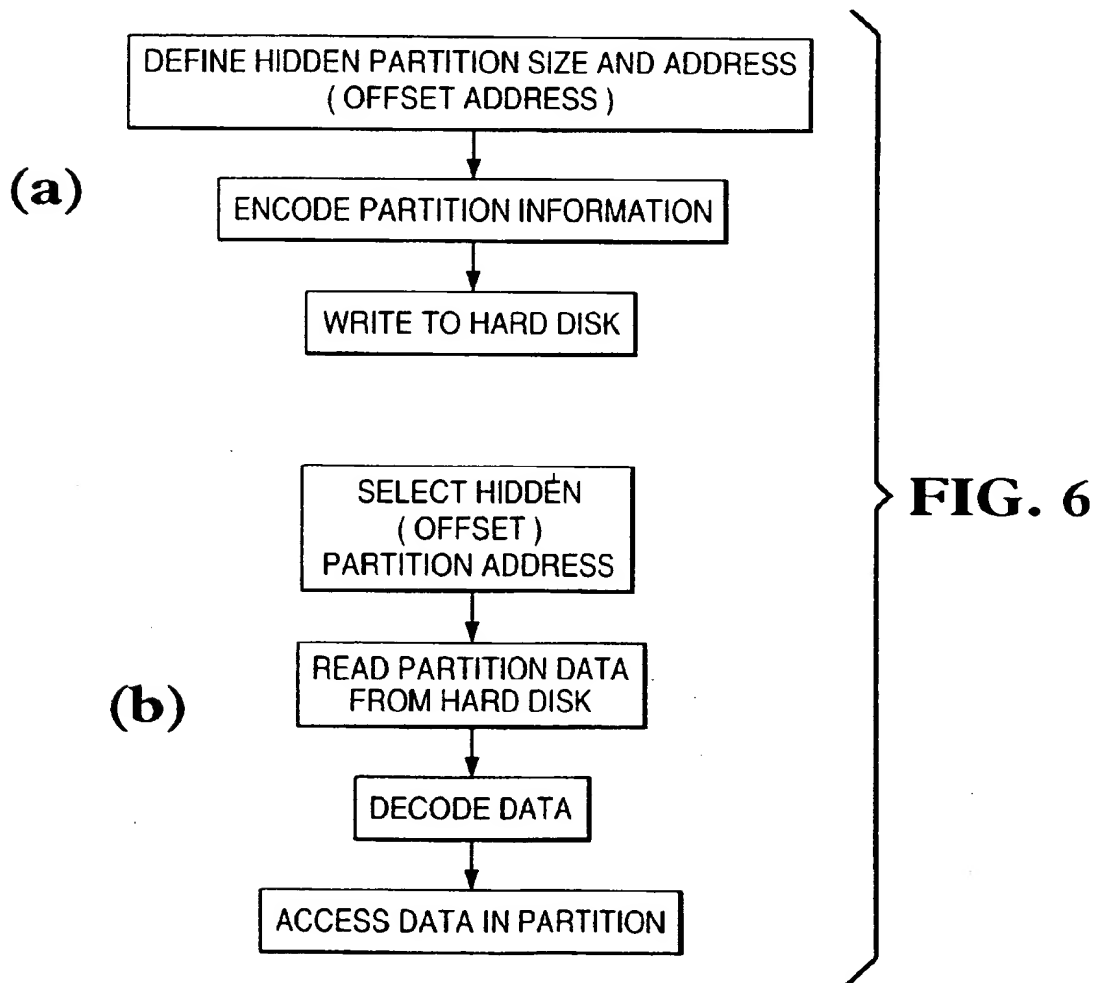
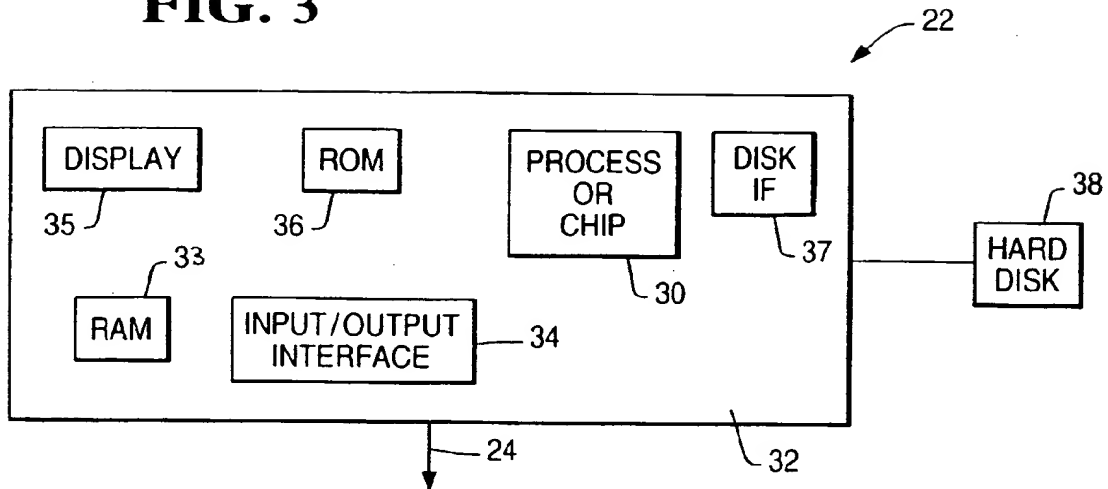


FIG. 3



00000000:	FA 33 C0 8E D0 BC 00 7C	- 8B F4 50 07 50 1F FB FC	3..... ...P.P...
00000010:	BF 00 06 B9 00 01 F2 A5	- EA 1D 06 00 00 BE BE 07	...< t. < u
00000020:	B3 04 80 3C 80 74 0E 80	- 3C 00 75 1C 83 C6 10 FE	u.....L
00000030:	CB 75 EF CD 18 8B 14 8B	- 4C 02 8B EE 83 C6 10 FE	t.< t.....< t.
00000040:	CB 74 1A 80 3C 00 74 F4	- BE 8B 06 AC 3C 00 74 0B	V.....^
00000050:	56 BB 07 00 B4 0E CD 10	- 5E EB F0 EB FE BF 05 00W...s.3
00000060:	BB 00 7C B8 01 02 57 CD	- 13 5F 73 0C 33 C0 CD 13	Ou..... .=
00000070:	4F 75 ED BE A3 06 EB D3	- BE C2 06 BF FE 7D 81 3D	U.u..... ..Invalid
00000080:	55 AA 75 C7 8B F5 EA 00	- 7C 00 00 49 6E 76 61 6C	partition table
00000090:	69 64 20 70 61 72 74 69	- 74 69 6F 6E 20 74 61 62	Error loading
000000A0:	6C 65 00 45 72 72 6F 72	- 20 6C 6F 61 64 69 6E 67	operating system.
000000B0:	20 6F 70 65 72 61 74 69	- 6E 67 20 73 79 73 74 65	Missing operating
000000C0:	6D 00 4D 69 73 73 69 6E	- 67 20 6F 70 65 72 61 74	system.....Y.....
000000D0:	69 6E 67 20 73 79 73 74	- 65 6D 00 00 80 18 59 12
000000E0:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 00 00
000000F0:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 00 00
00000100:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 00 00
00000110:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 00 00
00000120:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 00 00
00000130:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 00 00
00000140:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 00 00
00000150:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 00 00
00000160:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 00 00
00000170:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 00 00
00000180:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 00 00
00000190:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 00 00
000001A0:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 00 00
000001B0:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 00 00
000001C0:	01 00 06 3F BF 0B 3F 00	- 00 00 C1 3C 20 00 00 01	...?..?.....<
000001D0:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 00 00
000001E0:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 00 00
000001F0:	00 00 00 00 00 00 00 00	- 00 00 00 00 00 00 55 AAU

FIG. 4

FIG. 5K



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 30 4600

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.8)
X	WO 96 33458 A (LETTVIN JONATHAN D) 24 October 1996 (1996-10-24)	1,6	G06F1/00
A	* page 4, line 26 - page 5, line 8 * * page 9, line 13 - page 11, line 2; figures 1,2 *	2-5,7-10	
X	US 5 675 769 A (RUFF ERIC J ET AL) 7 October 1997 (1997-10-07) * column 25, line 67 - column 26, line 18 *	1,6	
X	EP 0 636 981 A (IBM) 1 February 1995 (1995-02-01) * column 8, paragraph 4; figure 4 *	1,6	
A	GB 2 244 583 A (TOKYO SHIBAURA ELECTRIC CO) 4 December 1991 (1991-12-04) * abstract; figures 1,2 *	9,10	
X	PATRICK COLBERT ET AL: "Partition Magic" BIG BLUE & COUSINS NEWSLETTER: THE NEWSLETTER OF THE GREATER VICTORIA PC USERS' ASSOCIATION- WEB EDITION, 'Online! vol. 15, no. 4, May 1997 (1997-05), pages 1-2, XP002118659 Retrieved from the Internet: <URL:www.pentire.bc.ca/{bigblue/may97nl/pmagic.htm}> 'retrieved on 1999-10-12! * page 1, paragraph 5 *	1,6	TECHNICAL FIELDS SEARCHED (Int.Cl.8) G06F
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 13 October 1999	Examiner Moens, R
CATEGORY OF CITED DOCUMENTS		T: theory or principle underlying the invention E: earlier patent document, but published on, or after the filing date D: document cited in the application L: document cited for other reasons &: member of the same patent family, corresponding document	
X: particularly relevant if taken alone Y: particularly relevant if combined with another document of the same category A: technological background O: non-written disclosure P: intermediate document			

EPO FORM 1603 03.02 (P04001)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 99 30 4600

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

13-10-1999

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9633458	A	24-10-1996	US 5559960 A	24-09-1996
			AU 5441796 A	07-11-1996
			US 5826012 A	20-10-1998
US 5675769	A	07-10-1997	AU 4986196 A	11-09-1996
			DE 19681257 T	26-02-1998
			EP 0811196 A	10-12-1997
			JP 10512379 T	24-11-1998
			WO 9626487 A	29-08-1996
			US 5706472 A	06-01-1998
			US 5930831 A	27-07-1999
EP 0636981	A	01-02-1995	JP 7044437 A	14-02-1995
			CA 2117393 A	27-01-1995
			CN 1111375 A	08-11-1995
			US 5666540 A	09-09-1997
GB 2244583	A	04-12-1991	JP 4031964 A	04-02-1992

EPO FORM P469

For more details about this annex: see Official Journal of the European Patent Office, No. 12/82